Secure Resource Allocation Protocol (SecRAP) for Time-Sensitive Networking

Lukas Osswald*, Steffen Lindner*, Lukas Bechtel†, Tobias Heer†, and Michael Menth*
*University of Tuebingen, Chair of Communication Networks, 72076 Tuebingen, Germany
†Esslingen University, Computer Science and Engineering, 73732 Esslingen, Germany
Email: {lukas.osswald, steffen.lindner, menth}@uni-tuebingen.de, {lukas.bechtel, tobias.heer}@hs-esslingen.de

***Abstract*—The convergence of operational technology (OT) and information technology (IT) networks through Time-Sensitive Networking (TSN) promises enhanced efficiency and new use cases in industrial settings. However, ensuring security in this shared infrastructure is crucial to prevent potential attacks that could compromise Quality of Service (QoS) of real-time streams and pose risks to operations and safety. This paper focuses on auditing the security of the Resource Allocation Protocol (RAP), a distributed QoS signaling protocol for TSN. We analyze the vulnerability of RAP to attacks during admission control, where end stations request network resources for data transmission. We leverage the Dolev-Yao attacker model to assess the security properties of RAP in both distributed hop-by-hop admission control and hybrid admission control with a central controller. We introduce novel security extensions to RAP, called Secure Resource Allocation Protocol (SecRAP), to mitigate the identified attack vectors. Finally, we present a prototype and discuss the security properties of SecRAP.**

I. Introduction

Common Industrial Ethernet (IE) protocols, e.g., PROFINET [17] and EtherCAT [20], implement deterministic data transmission and real-time control on the application layer. With this approach, different network protocols used in operational technology (OT) and information technology (IT) networks cannot share a common medium and must be operated on dedicated cables. Time-Sensitive Networking (TSN) is currently under standardization by the IEEE 802.1 TSN Task Group to enable the convergence of OT and IT networks. It enhances the Layer-2 Ethernet standard with mechanisms to guarantee real-time network services, e.g., bounded low latency or jitter, for higher-layer protocols. In the future, OT and IT network convergence will enable new use cases in which industrial machines communicate in real-time via traditional IT networks. As a result, IE and common IT protocols can be run via the same physical network infrastructure while preserving the QoS requirements for each TSN data flow, so-called streams. The shared physical network infrastructure imposes new and increased security requirements for protocols within the TSN network. In particular, the manipulation of QoS-guarantees in a network by an attacker can have a high impact with small, hard-to-detect changes. Such attacks can lower product quality, damage equipment, or even endanger human life. As a consequence, all protocols involved in TSN should consider security and privacy by design.

This work has been supported by the German Federal Ministry of Education and Research (BMBF) under support code 16KIS1161 (Collaborative Project KITOS). The authors alone are responsible for the content of the paper.

In this paper, we audit the security of the Resource Allocation Protocol (RAP) [12], which is a novel distributed QoS signaling protocol for TSN, standardized by the IEEE TSN Task Group. End stations, so-called talkers and listeners, communicate their QoS demands before transmitting data via RAP to the network, which is called admission control. During the admission control procedure, network devices, such as switches, reserve resources based on the signaled QoS requirements, e.g., they reserve a certain bandwidth for a TSN stream. Despite the criticality of admission control for the network, the current state of RAP does not implement any security measures. An attacker might degrade the QoS requirements of a TSN stream during the admission control procedure, replay old admission control requests, or claim all network resources by sending false admission control requests. The contribution of this paper is manyfold. First, we conduct a security analysis of the RAP protocol. We apply the commonly used Dolev-Yao attacker model [14] to analyze the security properties of RAP. We consider RAP in distributed hop-by-hop signaling via the so-called Edge Control Protocol (ECP) [6], which is an Ethernet-based flow control protocol that implements stop-and-wait automatic repeat request. Additionally, we analyze RAP in the hybrid model, in which RAP signaling is transported via TCP to a central controller. We define security properties to mitigate the identified attack vectors and present extensions to RAP, called Secure Resource Allocation Protocol (SecRAP), that fulfill the defined security properties. Thereby, we propose a novel LLDP-based mechanism to exchange IEEE 802.1AR device identifiers (DevIDs) between neighboring devices. Finally, we present a prototype of SecRAP.

The paper is structured as follows. Section II introduces TSN and admission control with RAP. Afterward, we review related work in Section III and analyze the security properties of RAP in Section IV. We propose extensions to RAP, called SecRAP, to mitigate the identified security issues in Section V. Section VI presents a prototype of SecRAP and discusses its security properties. Finally, we conclude the paper in Section VII.

©2024 29th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA24), September 2024, Padova, Italy

II. Background

In this section, we give an introduction to Time-Sensitive Networking (TSN) and admission control with RAP. Then, we give background information on identity management in industrial networks.

A. Time-Sensitive Networking

A TSN network consists of end stations and bridges. An end station is either a talker, sending data, or a listener, receiving data. In TSN, data flows are often referred to as streams. A stream originates from one talker and terminates at (multiple) listeners.

Bridges forward streams using one of TSN's traffic shaping mechanisms, e.g., Credit-Based Shaper (CBS) [3], Time-Aware Shaper (TAS) [4] or Cyclic Queuing and Forwarding (CQF) [5], to guarantee the requested network service. The applied mechanism is derived by the stream priority, which is encoded in the Priority Code Point (PCP) field in the VLAN header of the transmitted Ethernet packet. TSN streams have to be explicitly admitted to the network in a procedure called admission control. End stations signal[1] their communication needs, e.g., data rates and latency requirements, to the network. The network admits or denies a stream in either a distributed manner or with centralized control entities. IEEE Std 802.1Qcc [7] defines three strategies, also called configuration models, for admission control in TSN: the fully centralized, the fully distributed, and the centralized network/distributed user model.

1) The Fully Centralized Model: The fully centralized model uses central controllers, called Centralized User Configuration (CUC) and Centralized Network Configuration (CNC), to admit streams in the network. Signaling is done through non-IEEE standardized protocols, e.g., OPC UA [1]. Therefore, the fully centralized model is not discussed in this paper.

2) The Fully Distributed Model: The fully distributed model leverages a distributed admission control mechanism and is illustrated in Figure 1.

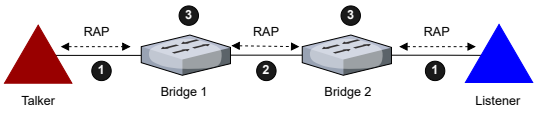


Figure 1: The fully distributed configuration model deploys a hop-by-hop based admission control procedure.

End stations signal their QoS requirements via the Resource Allocation Protocol (RAP) [12] in a hop-by-hop manner ❶ ❷. All bridges along the forwarding path take admission control decisions based on the signaled QoS requirements and local information ❸ and forward the RAP frames accordingly. In the fully distributed configuration model, RAP frames use ECP as transport protocol (see Section II-B for details).

[1]It is typically assumed that paths, as well as multicast addresses, are preconfigured in the network by other means.

3) The Centralized Network/Distributed User Model: The centralized network/distributed user model, also called *hybrid*, is a combination of the fully centralized and fully distributed configuration model. QoS requirements are signaled with a distributed protocol, and admission control is performed in a centralized manner. Figure 2 illustrates the centralized network/distributed user model.

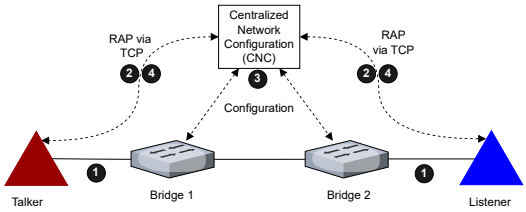


Figure 2: The centralized network/distributed user model combines centralized network management of the fully centralized and the distributed admission control protocol of the fully distributed configuration model.

End stations signal their QoS requirements via RAP ❶ ❷ directly to a centralized control entity, i.e., the CNC, via a TCP tunnel (see Section II-B for details). The CNC takes an admission control decision, configures the bridges in the network ❸, and notifies the end stations ❹ whether the stream is admitted or denied.

B. Admission Control with RAP

RAP is a novel protocol for distributed QoS signaling in TSN networks, currently under standardization in IEEE P802.1Qdd [12]. It is intended to be used in the fully distributed and centralized network/distributed user model. Figure 3 illustrates the protocol stack that is used for QoS signaling with RAP. The protocol stack is composed of RAP, LRP, and ECP or TCP.

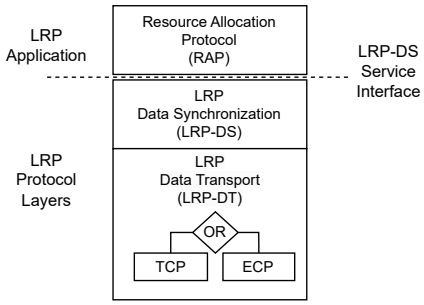


Figure 3: LRP stack with RAP as an LRP application.

1) Resource Allocation Protocol (RAP): RAP uses two[2] basic message formats, also called attributes, for QoS signaling and admission control in a network: Talker Announce Attribute

[2]For simplicity, we omit Resource Allocation Class Attribute (RACA) messages which are exchanged during RAP domain establishment.

(TAA) and Listener Attach Attribute (LAA). A talker signals its QoS requirements in a TAA. Similarly, a listener signals its QoS requirements in a LAA. Both TAA and LAA contain *mutable fields*, which are altered by each RAP-capable bridge along the forwarding path, and *constant fields*, which are set once by the end stations. An example of a mutual field is the status information contained in each LAA, which is updated if required by bridges. Additionally, fields can be added to extend an attribute, e.g., failure information fields are added to a TAA. An example of a constant field is the stream identifier, which is a unique eight-byte number used to identify the stream.

The existence of mutable fields and constant fields has implications on how the protocol can be integrity protected and authenticated. Details are discussed in Section IV.

2) Link-Local Registration Protocol (LRP): LRP [16] is a protocol suite to replicate and synchronize a database with up to 1 Mbyte between two neighboring peers. It is used by RAP to persistently store and transfer RAP attributes between bridges and end stations until they are actively revoked, or a connection failure is detected. RAP uses LRP's application interface to announce and revoke stream requests as RAP attributes.

LRP consists of two layers, the LRP Database Synchronization (LRP-DS) and the LRP Database Transport (LRP-DT). LRP-DS implements state machines for connection management and data transmission and reception. Further, it stores attributes announced by RAP and deletes attributes revoked by RAP. LRP-DT allows the use of two protocols for data transmission: Edge Control Protocol (ECP) and Transmission Control Protocol (TCP). ECP [6] is a simple link-local flow control protocol for Ethernet that implements a stop-and-wait automatic repeat request mechanism. It ensures reliable and in-order delivery of data between two Layer-2 peers. Additionally, LRP-DT can use TCP for data transport. With LRP-DT over TCP, data communication between two non-adjacent devices is possible. The security implications of ECP and TCP are further discussed in Section IV.

3) RAP in the Fully Distributed Model: Within the fully distributed model (see Figure 1), end stations signal their QoS requirements via RAP. Initially, talkers request a stream by sending a TAA including stream properties and QoS requirements. The attribute is transported with LRP-DT over ECP to the next RAP bridge. The bridges along the path of the stream forward the TAA in a hop-by-hop manner until it reaches the bridges connected to listeners.

Listeners request a stream by sending a LAA to the next RAP bridge. Similarly to a TAA, the LAA is sent using LRP-DT over ECP. If a bridge receives a matching TAA and LAA for a stream, the bridge checks the available resources for that stream and performs a local admission control procedure. When a stream is admitted, the bridge configures its traffic shaping accordingly. The LAA is forwarded with a success status in the direction of the talker. When a stream is declined or admitted, status information in the LAA is used to notify the Talker. Similarly, the TAA is used to notify the listeners about the failure by adding fields containing information about the error.

4) RAP in Centralized Network/Distributed User Model: Within the centralized network/distributed user model (see Figure 2) end stations signal their QoS requirements via RAP directly to the CNC through a TCP tunnel. This is achieved through a proxy mechanism of LRP, that establishes the TCP connection between the end station and the CNC. Details on the proxy mechanism can be found in [23].

C. Identity Management

Secure device communication requires unique identities to authenticate communicating parties. The IEEE 802.1 TSN Task Group specifies the TSN profile IEC/IEEE 60802 [2], which includes various mechanisms for network management, QoS, and security. It specifies the need for IEEE 802.1AR [27] device identifiers (DevIDs) to improve security in industrial networks. Figure 4 illustrates the device life-cycle of a device with an IEEE 802.1AR DevID.

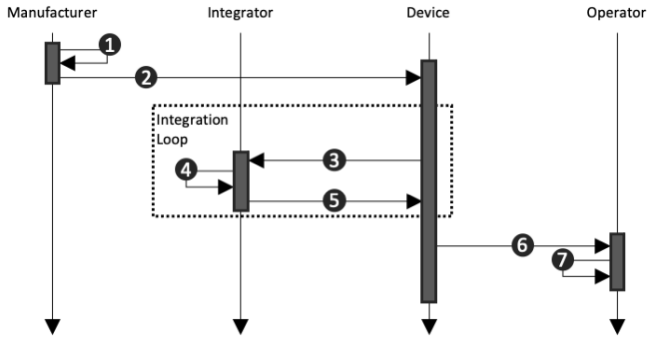


Figure 4: Device life-cycle of a device with an IEEE 802.1AR device identity.

During device manufacturing, the manufacturer generates a unique initial device identifier (IDevID) ❶ that contains an X.509 v3 certificate. The manufacturer signs the certificates with an official certificate from its own public key infrastructure (PKI). After generation, IDevIDs are stored in a security module on the device ❷. With the help of IDevIDs, integrators and operators can verify that a device has been produced by a specific vendor ❸. Additionally, signed firmware and secure boot can be protected with this identity. During the integration of a device in a larger machine, the integrator can trigger the generation of locally significant device identifiers (LDevIDs) signed by the certificate of the machine ❹. LDevIDs are also stored in a security module of the device ❺. With this approach, machine builders can generate machine certificate structures where all devices have certificates signed by the same machine root certificate. Similarly, multiple machines can be combined in a certificate infrastructure for a complete production line or factory. This hierarchical structure of integration is implemented through the *Integration Loop*, repeating

steps ❸ to ❺. Finally, the operator gathers the LDevIDs ❻, verifies them, and stores the discovered certificates for later use ❼.

III. Related Work

This section reviews related work regarding security of TSN networks, reservation protocols and identity management in industrial networks.

A. Security of Time-Sensitive Networking (TSN)

Ergenç et al. [15] analyzed the security of the landscape of TSN standards. Their overview paper identifies security risks in configurations of TSN features and protocols like admission control. Specifically, they identified security risks in IEEE 802.1Qat (SRP), the predecessor of RAP.

Rezabek et al. [25] analyze the security of Precision Time Protocol (PTP) and find that it lacks mechanisms for authentication and integrity protection. As a result, the authors extend PTP with a keyed-Hash Message Authentication Code (HMAC).

Peña et al. [24] analyze the impact of MACsec [8] on the forwarding performance of TSN traffic. Based on their analysis, the performance of MACsec does not limit its applicability in TSN networks. Dik et al. [13] develop a MACsec TSN architecture to support frame-preemption with MACsec. This increases the applicability to most TSN network architectures. However, MACsec can only protect single links and does not provide end-to-end protection for stream reservation protocols. Additionally, the initial configuration of MACsec is complex and requires hardware support making backward compatibility difficult.

B. Security of Resource Reservation Protocol (RSVP)

Resource allocation and reservation is a well-known problem in communication networks. For example, RSVP [9], a well-established protocol for IP-based networks, includes security properties for user authentication, integrity protection, and node authentication. The mechanisms include hop-by-hop and replay protection, as described in RFC2747 [21]. RFC4230 [18] summarizes and explains these security properties. This detailed explanation also includes problems and open points in the deployment of RSVP. For example, the selection of modern cryptography, security settings for authentication, the key distribution, or path selection require to be solved in advance. Hence, the creation of secure ad-hoc RSVP reservation is difficult.

C. Identity Management in OPC UA

The OPC UA Part 21 [22] specification defines a lifecycle for certificates in machines and factories. The OPC UA model defines multiple stages with manufacturing, distribution, assembly, and operation, similar to IEEE 802.1AR [27] (see Section II-C). In each of these stages, the OPC UA model allows the transfer of a root certificate to the new owner of a device or set of devices. All devices keep their original identities and trust only the new hierarchy. OPC UA is typically used for resource reservation and admission control in fully centralized TSN domains.

IV. Security Analysis of RAP

This section presents a threat analysis of RAP and defines security properties to mitigate the findings. We first introduce the used attacker model and present possible attack scenarios that illustrate security issues. Then, we define security properties to prevent the presented attack scenarios.

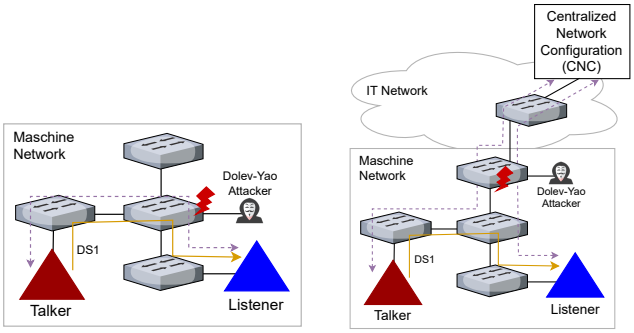
A. Threat Model

Failures due to attacks in industrial control systems can cause physical damage to machines and human operators. Due to the extent of possible harm, all protocols involved in TSN should follow a security-by-design paradigm.

The Dolev-Yao attacker model [14] is commonly used for analyzing network protocol security and is considered very powerful [11]. In the model, the attacker can alter and replay messages and impersonate any device but cannot break encryption. Thus, the model is a suitable choice for analyzing protocols used in critical infrastructure to provide a high-security level. In the context of TSN and RAP, a Dolev-Yao attacker can impersonate end stations to inject RAP packets. Furthermore, the Dolev-Yao attacker can impersonate bridges to alter values in RAP packets or perform replay attacks with old admission control requests. In this work, we only analyze the security of RAP. Attack vectors enabled by other protocols are out of scope of this work.

B. Threat Analysis

In this section, we conduct the threat analysis for both configuration models of TSN with RAP: 1) the fully distributed model and 2) the hybrid model. The example networks are illustrated in Figures 5(a)–5(b). In general, we assume the attacker to be as powerful as defined in the Dolev-Yao model, but as state-of-the-art RAP does not provide any security measures, in some cases, simpler attacks are sufficient.



(a) Network using distributed admission control.

(b) Network using centralized admission control.

Figure 5: Example networks with Dolev-Yao attacker.

1) Fully Distributed QoS Signaling using RAP: Figure 5(a) shows a TSN network that uses the fully distributed admission control via RAP. End stations exchange signaling messages with the network. Each bridge along the signaling path admits the stream based on local information and notifies all participants about the reservation's status. With fully distributed signaling, the signaling path and data path are identical.

a) Denial of Service: An attacker can forge RAP requests to reserve resources that are not intended to be used. As a result, other streams may be denied due to an apparent lack of resources. A more subtle denial of service attack can be achieved by changing the stream identifiers included in RAP messages. As a result, bridges up- and downstream from the attacker could not match the talker with listener requests. Therefore, the stream requests cannot be processed by a bridge. An application requesting resources would either wait infinitely or report an error state to an operator after a timeout, causing disruption in production.

b) QoS Degradation: Another attack is the impersonation of a bridge to manipulate incoming signaling messages by talkers and listeners of the same stream. Depending on the manipulated fields, such an attack can have various impacts on the provided QoS service by the network. An attacker might change a data stream's traffic description, e.g., the data rate or latency requirement. Inducing a stricter latency requirement for each manipulated stream leads to more network overhead, which, over time, can lead to a denial of service attack. Softening latency requirements is even more critical in this attack. In that case, the network does not guarantee the latency requested by the end stations, leading to unpredictable machine behavior that can halt production or even endanger human operators. Attacks involving the manipulation of traffic parameters are particularly difficult to detect because small changes can have a big impact on the network.

c) Replay Attacks: Simple in-session replay attacks are prevented by the sequence numbers of LRP when using RAP over ECP. However, those sequence numbers are not protected by cryptographic algorithms and, thus, can be manipulated. Additionally, the LRP handshake for connection establishment does not include sequence numbers and thus can be disrupted [16].

2) Hybrid QoS Signaling using RAP: Figure 5(b) shows a TSN network that uses hybrid admission control via RAP. In the hybrid model, end stations exchange RAP messages with a CNC via a TCP tunnel. Signaling messages are only forwarded by bridges but not processed for admission control. The signaling path may deviate from the data path, as the CNC may be located anywhere in the network. Therefore, bridges along the signaling path that are not involved in admission control can eavesdrop on the admission control procedure. An attacker located in an IT network on the path to the CNC can use the signaling information for reconnaissance of an internal machine network. Additionally, an attacker that is not part of the signaling path can use ARP-spoofing to be a person-in-the-middle attack and manipulate the QoS signaling similarly as in the fully distributed model. This can enable an attacker to spread an attack to the machine level, even without physical access to the machine network. Replay attacks are possible if the TCP sequence numbers are modified accordingly.

C. Security Properties

In the following, we define desirable security properties that should hold for RAP to prevent the discussed attacks. We present SecRAP as an extension to RAP that fulfills all defined security properties in Section V.

1) Authentication: Authentication is the process of verifying the identity of a device before granting access to a service. For RAP signaling, this means that devices need to authenticate each other before engaging in RAP communication. Authentication prevents an attacker from forging new admission control requests. RAP does not implement any method for the network to authenticate end stations. We propose a novel method for identity management and distribution of X.509 certificates in Section V-B.

2) Non-repudiation: Non-repudiation is a property that assures that the authorship of a packet cannot be denied by the author. For RAP this means that resource reservations can be undeniably linked to the end station requesting the resources. Currently, RAP does not provide non-repudiation.

3) Integrity: Integrity protection is a method to ensure that packet data is not altered by unauthorized devices. With integrity protection, an attacker is unable to degrade the requested QoS during the admission control procedure or to change the stream identifier in RAP message. Currently, RAP does not provide integrity protection.

4) Confidentiality: Confidentiality protects messages from unauthorized reading access. RAP messages that are transported via ECP do not require confidentiality, as all bridges along the path take part in the admission control decision. RAP messages transmitted via TCP are forwarded by bridges that are not involved in admission control. Therefore, confidentiality must be guaranteed to prevent reconnaissance of internal machine networks.

V. Secure Resource Allocation Protocol (SecRAP)

This section introduces extensions to RAP, called Secure Resource Allocation Protocol (SecRAP), to mitigate the identified attacks from Section IV. First, we define general components of SecRAP, i.e., identity discovery, hop-by-hop protection, and end-to-end protection. Then, we discuss the details of the individual components.

A. Components of Secure Resource Allocation Protocol (SecRAP)

SecRAP implements the security properties of Section IV-C: authentication, non-repudiation, integrity, and confidentiality.

The foundation of these properties is a unique **identity discovery**, which represents the first component of SecRAP. Further, integrity, non-repudiation, and confidentiality can be implemented on different layers, i.e., **hop-by-hop** or **end-to-end**. Hop-by-hop protection is the second, and end-to-end protection the third component of SecRAP. Figure 6 shows an architectural overview of SecRAP that uses the three components identity discovery, hop-by-hop protection, and end-to-end protection.

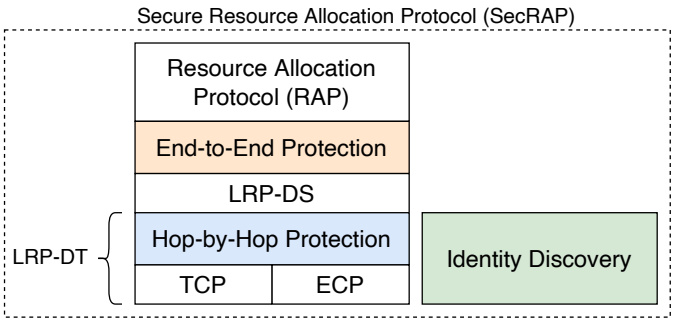


Figure 6: Secure Resource Allocation Protocol (SecRAP) architecture consisting of the three components: 1) identity discovery, 2) hop-by-hop protection, and 3) end-to-end protection.

Identity discovery is the foundation for all authentication and cryptographic operations in SecRAP. Hop-by-hop protection is used to secure the communication between two LRP peers, i.e., in the case of RAP over ECP between two adjacent devices and in the case of RAP over TCP between an end station and the CNC. End-to-end protection is used to protect the communication between two end stations, i.e., a talker and a listener.

B. Identity Discovery

The basis for secure RAP signaling is an identity discovery mechanism between two LRP peers. We propose to use 802.1AR DevIDs, i.e., IDevIDs and LDevIDs, for device identification. To that end, each device generates a LDevID that uniquely identifies the device, i.e., it contains additional information such as serial number and used MAC addresses, signed by the PKI of the operator or factory. We propose to use XLLDP[3] [19], an extension of LLDP, to exchange X.509 certificate chains (LDevIDs) between two neighbors. We define a new Type-Length-Value (TLV) to transfer the certificate of a device and the complete certificate chain to its neighbor. Figure 7 illustrates how a device can verify the validity of a neighbor certificate.

All devices in the network, i.e., all end-devices and bridges, send their LDevID certificate with the complete certificate chain via Extended Link Layer Discovery Protocol (XLLDP) to all neighbors ❶. When a device receives a certificate from its neighbor, it can verify it by using the attached certificate chain and the trusted root certificate of the operator or factory ❷. Every device stores the verified certificate of its neighbor until the neighbor is disconnected.

[3]X.509 certificates are too large for default LLDP.

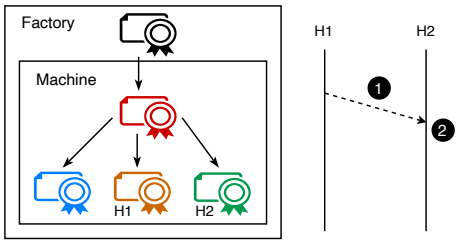


Figure 7: Exchange of LDevID certificates using XLLDP between two peers H1 and H2.

C. Hop-by-Hop Protection

Hop-by-hop protection ensures that two LRP peers communicate over a secure channel. This includes integrity protection, i.e., the packet data cannot be altered by unauthorized devices, and optionally confidentiality and non-repudiation.

1) RAP over ECP: With RAP over ECP, RAP frames are transported in a hop-by-hop manner, and all bridges along the forwarding path take part in the admission control procedure. We propose to adopt TLS to ECP and call it ETLS to differentiate it from the original TLS typically associated with TCP. ETLS enables integrity protection as described in the Integrity-Only Cipher Suite of TLS 1.3 in RFC 9150 [10]. Specifically, ETLS is based on a HMAC over the ECP data unit, i.e., the LRP packet. Confidentiality is not needed with ECP because all devices on the signaling path must read the packet content.

The discovered LDevID certificates are used to authenticate a Diffie-Hellmann (DH) key exchange as in TLS 1.3. On the sending side, an ETLS-enabled ECP implementation computes the HMAC over the ECP data unit with the shared secret and appends the Message Authentication Code (MAC) to an ETLS header, including a 64-bit sequence number for replay protection as in TLS 1.3. On the receiving side, an ETLS-enabled ECP implementation computes the HMAC over the ECP data unit with the shared secret and compares it with the attached MAC of the ETLS header. If the attached MAC and the computed HMAC are the same, then it is ensured that the packet has not been altered by an attacker.

2) RAP over TCP: With RAP over TCP, RAP frames are transported from an end station to a CNC via a TCP tunnel. The state-of-the-art security layer to secure TCP is Transport Layer Security (TLS). We propose to secure RAP over TCP with TLS 1.3 using the X.509 certificates within the LDevIDs. The identities are used for client-server authentication of the TLS handshake. Keys for encryption and integrity protection can be automatically exchanged via DH. As a result, all RAP communication over TCP with TLS is confidential,

authenticated, and integrity-protected between an end station and the CNC. Non-repudiation can be optionally added using a TLS extension called TLS-N [26].

D. End-to-End Protection

Hop-by-hop protection only ensures secure communication between two LRP peers and prevents transparent person-in-the-middle attacks. For example, a corrupted bridge may still be able to degrade the requested QoS within a RAP message after ETLS validation by decreasing the requested bandwidth. RAP messages contain mutable fields, e.g., status fields, and constant fields, e.g., stream identifiers and data rate. Mutable fields are automatically protected by ETLS/TLS between two LRP peers. We propose to use a signature algorithm based on asymmetric cryptography, such as ECDSA, to end-to-end protect constant fields against manipulation. Figure 8 illustrates the proposed mechanism for a Listener Attach Attribute (LAA) RAP message.

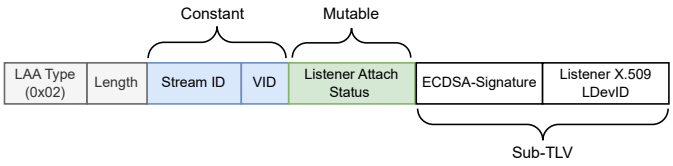


Figure 8: RAP attribute of a Listener extended by an end-to-end protection TLV using ECDSA signatures and the LDevID of the listener.

The listener creates a hash, e.g., SHA-256, over the constant fields of the RAP message and signs the hash with its X.509 certificate from its LDevID[4]. The X.509 certificate, signed by the PKI of the operator, is attached to the RAP message as a TLV. All bridges and end stations along the forwarding path are able to validate the integrity of the RAP message and can detect manipulation by an attacker. We recommend the use of ECDSA to reduce the key size while keeping the same level of security. As ECDSA validation is computationally expensive and introduces a large overhead compared to symmetric cryptography, end-to-end protection is optional within SecRAP.

VI. Prototype and Discussion of SecRAP

In this section, we present a prototype for the presented hop-by-hop and end-to-end protection of SecRAP. Further, we discuss SecRAP's security properties.

A. Prototype

We implemented and validated the proposed hop-by-hop and end-to-end protection of SecRAP as a proof-of-concept. The implementation is publicly available on Github[5].

[4]The certificate needs to contain information that is unique to the talker, e.g., MAC addresses.

[5]https://github.com/uni-tue-kn/SecRAP

1) End-to-End Protection: We implemented the proposed end-to-end integrity header of RAP with a user space program in Python. There, the certificate of the LDevID is attached to the RAP message, and a hash of the constant fields is computed. Finally, the hash is signed with ECDSA. A receiving RAP node then verifies the integrity of the constant RAP message fields with the attached certificate that is signed by the factory and identifies the talker/listener.

2) Hop-by-Hop Protection: We implemented[6] the proposed ETLS mechanism with extended Berkeley Packet Filter (eBPF) in the Linux kernel. eBPF is a mechanism that allows the execution of isolated programs at different levels in the Linux kernel, so-called hooks. Therefore, it is well suited to extend the Linux kernel with transparent packet processing logic. The processing logic of our eBPF-prototype is shown in Figure 9.

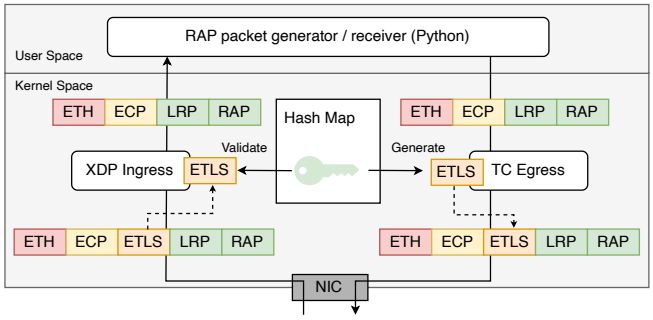


Figure 9: Processing path of the eBPF-based prototype for integrity-protected ECP with a keyed-Hash Message Authentication Code (HMAC).

The eBPF program processes the generated RAP messages from our Python program (see Section VI-A1). It attaches itself to the traffic control (tc) hook of the Linux kernel, which is executed when a packet is transmitted through an interface. If the packet is an ECP packet, the eBPF program computes the HMAC and attaches an ETLS header with the computed MAC including a 64-bit sequence number. Further, the eBPF program attaches itself to the so-called XDP hook of the Linux kernel, which is executed when a packet is received on an interface. If an ECP-ETLS packet is received, the HMAC is computed and compared to the attached MAC in the ETLS header. If the packet is valid, the ETLS header (including the MAC) is removed and passed to the user space. Otherwise, the packet is dropped.

B. Discussion

Table I summarizes the security properties of RAP and SecRAP.

The desirable security properties of Section IV-C, i.e., authentication, non-repudiation, integrity, and confidentiality, are

[6]For simplicity, our prototype assumes a pre-shared secret for HMAC computation.

Table I: Security properties implemented by SecRAP.
(✓= supported/protected, (✓) = optional, × = not supported)

Security Property	RAP over ECP	RAP over TCP	SecRAP over ECP	SecRAP over TCP
Authentication	×	×	✓	✓
Non-repudiation	×	×	(✓)	(✓)
Integrity	×	×	✓	✓
Confidentiality	×	×	×	✓
Denial of Service	×	×	✓	✓
QoS Degradation	×	×	✓	✓
Replay Attack	✓	✓	✓	✓

not met by state-of-the-art RAP. With SecRAP over ECP, authentication is provided by X.509 certificates (LDevIDs), and non-repudiation is optionally achieved by ECDSA signatures of the end-to-end protection header. Integrity is protected with ETLS, and confidentiality is not required. With SecRAP over TCP, authentication is provided by TLS with X.509 certificates (LDevIDs), and non-repudiation is optionally achieved with TLS-N [26]. Integrity and confidentiality are provided by TLS.

RAP is prone to most of the identified attack vectors of Section IV-B. Simple in-session replay attacks are prevented by the sequence numbers of ECP/TCP. In contrast, SecRAP is protected against all identified attack vectors.

The proposed solution adds overhead to RAP packets and processing time. Admission control happens before a stream is sent, thus the network load is little. Therefore, the overhead of SecRAP is negligible. The delay and bandwidth of a reserved stream is not impacted by SecRAP.

VII. Conclusion

In this paper, we conducted a security analysis of RAP using the Dolev-Yao attacker model. We identified several attack vectors that enable denial of service, QoS degradation and replay attacks. Based on our findings, we defined desirable security properties for secure admission control in TSN. We proposed extensions to RAP, called SecRAP, to mitigate the presented attack vectors. SecRAP introduced three components for secure admission control in TSN: identity discovery, hop-by-hop protection, and end-to-end protection. We presented a novel identity discovery mechanism based on LLDP to exchange X.509 certificates (LDevIDs) between neighboring devices. The exchanged certificates are used to secure hop-by-hop communication with RAP over ECP. Additionally, we proposed a security header extension to RAP to implement end-to-end integrity protection with ECDSA. Finally, we presented a proof-of-concept implementation for SecRAP and discussed its security properties.

References

[1] OPC Foundation. https://opcfoundation.org/. Accessed: 2024-04-25.

[2] IEC/IEEE Time-Sensitive Networking Profile for Industrial Automation. *IEC/IEEE 60802*, 2002.

[3] IEEE Standard for Local and Metropolitan Area Network–Virtual Bridged Local Area Networks – Amendment 12: Forwarding and Queueing Enhancements for Time-Sensitive Streams. *IEEE Std 802.1Qav*, 2009.

[4] IEEE Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks – Amendment 25: Enhancements for Scheduled Traffic. *IEEE Std 802.1Qbv*, 2015.

[5] IEEE Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks – Amendment 29: Cyclic Queuing and Forwarding. *IEEE Std 802.1Qch*, 2017.

[6] IEEE Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks. *IEEE Std 802.1Q-2018*, 2018.

[7] IEEE Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks – Amendment: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements. *IEEE Std 802.1Qcc*, 2018.

[8] IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security. *IEEE Std 802.1AE*, pages 1–239, 2018.

[9] Robert T. Braden, Lixia Zhang, Steven Berson, Shai Herzog, and Sugih Jamin. Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification. RFC 2205, September 1997.

[10] N. Cam-Winget and J. Visoky. RFC 9150 TLS 1.3 Authentication and Integrity-Only Cipher Suites, 2022.

[11] Iliano Cervesato. The Dolev-Yao intruder is the most powerful attacker. In *Symposium on Logic in Computer Science (LICS)*, volume 1, pages 1–2, 2001.

[12] Feng Chen. IEEE Draft Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks – Amendment: Resource Allocation Protocol. *IEEE P802.1Qdd Draft 0.9*, 2024.

[13] Daniel Dik, Iacob Larsen, and Michael Stübert Berger. MACsec and AES-GCM Hardware Architecture with Frame Preemption Support for Transport Security in Time Sensitive Networking. In *International Conference on Computer, Information and Telecommunication Systems (CITS)*, pages 01–07, 2023.

[14] Danny Dolev and Andrew Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[15] Doğanalp Ergenç, Cornelia Brülhart, Jens Neumann, Leo Krüger, and Mathias Fischer. On the Security of IEEE 802.1 Time-Sensitive Networking. In *IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6, 2021.

[16] Norman Finn. IEEE Draft Standard for Local and Metropolitan Area Network–Link-local Registration Protocol. *IEEE Std 802.1CS*, 2020.

[17] Friesen, A and Schriegel, S and Biendarra, A. PROFINET over TSN Guideline Version 1.21. *Profibus International (PI), Profibus International (PI)*, 2021.

[18] Richard F. Graveman and Hannes Tschofenig. RSVP Security Properties. RFC 4230, December 2005.

[19] Stephen Haddock. IEEE Standard for Local and metropolitan area networks–Station and Media Access Control Connectivity Discovery Amendment 2: Support for Multiframe Protocol Data Units. *IEEE Std 802.1ABdh*, 2021.

[20] International Electrotechnical Commission (IEC). IEC 61158-1. *Industrial communication networks - Fieldbus specifications - Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series*, 2023.

[21] Bob Lindell, Fred Baker, and Mohit Talwar. RSVP Cryptographic Authentication. RFC 2747, January 2000.

[22] OPC Foundation. OPC Unified Architecture Specification Part 21: Device Onboarding. 2022.

[23] Lukas Osswald, Steffen Lindner, Lukas Wüsteney, and Michael Menth. RAP Extensions for the Hybrid Configuration Model. In *IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–8, September 2021.

[24] Roger Antonio Peña, Mikel Pascual, Armando Astarloa, Daniel Uribe, and Jon Inchausti. Impact of MACsec security on TSN traffic. In *Conference on Design of Circuits and Integrated Circuits (DCIS)*, pages 01–06, 2022.

[25] Filip Rezabek, Max Helm, Tizian Leonhardt, and Georg Carle. Ptp Security Measures and their Impact on Synchronization Accuracy. In *International Conference on Network and Service Management*, pages 109–117, 2022.

[26] Hubert Ritzdorf, Karl Wust, Arthur Gervais, Guillaume Felley, and Srdjan Capkun. TLS-N: Non-repudiation over TLS enabling ubiquitous content signing. In *Network and Distributed System Security Symposium (NDSS)*, 2018.

[27] Mick Seaman. IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity. *IEEE Std 802.1AR*, 2018.